Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - ASPjar Guestbook SQL Injection
  - Access Remote PC Password Disclosure
  - Acoo Browser Javascript Spoofing
  - AM Browser Javascript Spoofing
  - Community Server Cross Site Scripting
  - Crazy Browser Javascript Spoofing
  - Golden FTP Server File and Path Disclosure
  - GoSurf Browser Javascript Spoofing
  - IISWorks.com ASP KnowledgeBase Database Disclosure
  - IISWorks.com ASP Webmail Database Disclosure
  - IISWorks.com Fileman Database Disclosure
  - IISWorks.com ListPics Database Disclosure
  - Hitachi Multiple Hibun Products Security Restriction Bypass
  - K-Meleon Denial of Service
  - McAfee IntruShield Security Management System Cross Site Scripting & Information Disclosure
  - Microsoft FrontPage Denial of Service
  - Microsoft Internet Explorer Arbitrary Code Execution
  - Microsoft Internet Information Server HTTP Response Smuggling
  - Microsoft Windows NTFS File Block Initialization
  - **Microsoft Windows Message Queuing Remote Code Execution Vulnerability (Updated)**
  - Netscape Denial of Service
  - NotJustBrowsing Browser Javascript Spoofing
  - Prevx Pro File Modification & Driver Spoofing
  - SSH Secure Shell and Tectia Server Key Disclosure
  - TCP Chat Denial of Service
  - **Veritas Backup Exec Multiple Vulnerabilities (Updated)**
- UNIX / Linux Operating Systems
  - Adobe Acrobat Reader UnixAppOpenFilePerform Buffer Overflow
  - Adobe Reader For Unix Local File Disclosure
  - **Bzip2 Remote Denial of Service (Updated)**
  - **BZip2 File Permission Modification (Updated)**
  - CenterICQ Insecure Temporary File
  - Crip Helper Script Insecure Temporary File Creation
  - Clam Anti-Virus ClamAV Remote Denials of Service
  - Courier Mail Server Remote Denial of Service
  - **Ettercap Remote Format String (Updated)**
  - Log4sh Insecure Temporary File Creation
  - FreeBSD ipfw Packet Lookup Firewall Bypass
  - FreeBSD TCP Stack Established Connection Remote Denial of Service
  - Geeklog User Comment Retrieval SQL Injection
  - GlobalNoteScript 'Read.CGI' Remote Command Execution
  - GNU GNATS Gen-Index Arbitrary Local File Disclosure/Overwrite
  - **GNU GZip Directory Traversal (Updated)**
  - **GNU GZip File Permission Modification (Updated)**
  - KPopper Insecure Temporary File Creation
  - **Multiple Vendors Apple Safari Remote Code Execution (Updated)**
  - Multiple Vendors TLS Plaintext Password
  - Multiple Vendors Zlib Compression Library Buffer Overflow
  - NetBSD CLCS / EMUXKI Audio Driver Local Denial of Service
  - Net-SNMP Protocol Denial Of Service
  - OFTPD User Command Buffer Overflow
  - PHPPGAdmin Login Form Directory Traversal
  - Eskuel Unauthorized Administrator Access
  - RaXnet Cacti Multiple Vulnerabilities
  - **Rob Flynn Gaim Remote Denial of Services (Updated)**
  - **Royal Institute of Technology Heimdal TelnetD Remote Buffer Overflow (Updated)**
  - **Sendmail Milter Remote Denial of Service (Updated)**
  - **Sun Solaris Runtime Linker 'LD_AUDIT' Elevated Privileges (Updated)**

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service

(DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
ASPJar Guestbook	An input validation vulnerability has been reported in ASPjar Guestbook that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	ASPjar Guestbook SQL Injection	High	Security Focus, ID: 12521, July 4, 2005
Access-Remote-PC Access Remote PC V4.5.1	A vulnerability has been reported in Access Remote PC that could let local malicious users disclose passwords. No workaround or patch available at time of publishing. There is no exploit code required.	Access Remote PC Password Disclosure	Medium	Security Tracker Alert ID: 1014377, July 5, 2005
Acoo Acoo Browser V1.17	A javascript spoofing vulnerability has been reported in Acoo Browser that could let remote malicious users spoof Javascript dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Acoo Browser Javascript Spoofing	Medium	Security Tracker Alert ID: 1014311, June 28, 2005
AMBrowser AM Browser V2.0.0	A javascript spoofing vulnerability has been reported in AM Browser that could let remote malicious users spoof Javascript dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	AM Browser Javascript Spoofing	Medium	Security Tracker Alert ID: 1014314, June 28, 2005
Community Server Community Server V1.1.0.50517	An input validation vulnerability has been reported in Community Server that could let remote malicious users perform Cross-Site Scripting. Update to version 1.1.0.50615, A proof of concept exploit has been published.	Community Server Cross Site Scripting CAN-2005-2084	High	Security Tracker Alert ID: 1014316, July 2, 2005
Crazy Browser Crazy Browser V2.0.0	A javascript spoofing vulnerability has been reported in Crazy Browser that could let remote malicious users spoof Javascript dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Crazy Browser Javascript Spoofing	Medium	Security Tracker Alert ID: 1014315, June 28, 2005
Golden FTP Server GoldenFTP Server V2.60	A vulnerability has been reported in Golden FTP Server that could let a remote malicious user uncover files and installation paths. No workaround or patch available at time of publishing. There is no exploit code required.	Golden FTP Server File and Path Disclosure CAN-2005-2142	Low	Secunia, Advisory: SA15840, July 1, 2005
GoSurf GoSurf Browser V2.54	A javascript spoofing vulnerability has been reported in GoSurf Browser that could let remote malicious users spoof Javascript dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	GoSurf Browser Javascript Spoofing	Medium	Security Tracker Alert ID: 1014313, June 28, 2005
IISWorks.com ASP KnowledgeBase V2.0g	A vulnerability has been reported in ASP KnowledgeBase that could let remote malicious users obtain database access, including administrative passwords. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ASP KnowledgeBase Database Disclosure	High	Security Tracker Alert ID: 1014384, July 5, 2005
IISWorks.com ASP Webmail V3.6c	A vulnerability has been reported in ASP Webmail that could let remote malicious users obtain database access, including administrative passwords. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ASP Webmail Database Disclosure	High	Security Tracker Alert ID: 1014385, July 5, 2005
IISWorks.com Fileman V6.5	A vulnerability has been reported in Fileman that could let remote malicious users obtain database access, including administrative passwords. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Fileman Database Disclosure	High	Security Tracker Alert ID: 1014383, July 5, 2005

IISWorks.com ListPics 4.1	A vulnerability has been reported in ListPics that could let remote malicious users obtain database access, including administrative passwords. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ListPics Database Disclosure	High	Security Tracker Alert ID: 1014378, July 5, 2005
Hitachi Hibun Advanced Edition Server 6.x, 7.x, Hibun Advanced Information Cypher 6.x, 7.x	Several vulnerabilities have been reported: a vulnerability was reported due to an error that causes PCMCIA hard disks that are attached to a system to be incorrectly treated as internal hard disks, which could let a malicious user bypass security restrictions; and a vulnerability was reported due to an error in the Hibun Viewer, which could let a malicious user bypass security restrictions. Updates available at: http://www.hitachi-support.com/security_e/vuls_e/HS05-011_e/index-e.html Currently we are not aware of any exploits for these vulnerabilities.	Hitachi Multiple Hibun Products Security Restriction Bypass	Medium	Secunia Advisory: SA15863, June 30, 2005
K-Meleon K-Meleon Browser V0.9	An empty javascript function processing vulnerability has been reported in K-Meleon Browser that could let remote malicious users perform a Denial of Service. As a workaround disable Javascript. A Proof of Concept exploit has been published.	K-Meleon Denial of Service	Low	Security Tracker Alert ID: 1014349, July 1, 2005
McAfee IntruShield Security Management	A vulnerability has been reported in IntruShield Security Management that could let malicious users perform Cross-Site Scripting or disclose authorized information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	IntruShield Security Management System Cross Site Scripting & Information Disclosure	High	Security Focus, ID: 14167, July 6, 2005
Microsoft Microsoft FrontPage XP	A vulnerability has been reported in FrontPage that could let malicious users crash the application. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft FrontPage Denial of Service CAN-2005-2143	Low	Security Tracker Alert ID: 1014352, July 1, 2004
Microsoft Microsoft Internet Explorer Internet Explorer V6SP2 on Windows XP Internet Explorer V6SP1 for Windows XP 64-Bit Internet Explorer V6SP1 for Microsoft Windows Server 2003 Internet Explorer V6SP1 on Microsoft Windows 98, 98 SE, Millennium Edition	A COM object (javaprxy.dll) exception handling vulnerability has been reported in Internet Explorer that could let remote malicious users perform arbitrary code execution or cause a Denial of Service. Microsoft has published workarounds, http://www.microsoft.com/technet/security/advisory/903144.mspx A Proof of Concept exploit script has been published.	Microsoft Internet Explorer Arbitrary Code Execution CAN-2005-2087	High	Microsoft Security Advisory 903144, June 30, 2005 **US-CERT VU#939605**
Microsoft Microsoft Internet Information Server V5.0, 6.0	A vulnerability has been reported in Internet Information Server that could let a remote malicious user perform HTTP Response Smuggling Attacks. No workaround or patch available at time of publishing. There is no exploit code required.	Microsoft Internet Information Server HTTP Response Smuggling CAN-2005-2089	Low	Security Tracker Alert ID: 1014364, July 3, 2005
Microsoft Microsoft Windows XP, Server, & 2000	An NTFS file block initialization vulnerability has been reported in Windows that could let malicious users reveal previous data. No workaround or patch available at time of publishing. There is no exploit code required.	Microsoft Windows NTFS File Block Initialization	Low	Security Focus, ID: 7386, June 30, 2005
Microsoft Windows 2000 SP 3 and SP4 Windows XP SP1 Windows XP 64-Bit Edition SP1 Windows 98 and 98 SE	A buffer overflow vulnerability has been reported that could let a remote malicious user execute arbitrary code. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-017.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Message Queuing Remote Code Execution Vulnerability CAN-2005-0059	High	Microsoft Security Bulletin MS05-017, April 12, 2005 **US-CERT VU#763513**

Netscape Netscape V8.0.2	An empty javascript function processing vulnerability has been reported in Netscape that could let remote malicious users perform a Denial of Service. As a workaround disable Javascript. A Proof of Concept exploit has been published.	Netscape Denial of Service	Low	Security Tracker Alert ID: 1014349, July 1, 2005
NotJustBrowsing NotJustBrowsing Browser V1.0.4	A javascript spoofing vulnerability has been reported in NotJustBrowsing Browser that could let remote malicious users spoof Javascript dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	NotJustBrowsing Browser Javascript Spoofing	Medium	Security Tracker Alert ID: 1014312, June 28, 2005
Prevx Prevx Pro 2005	A vulnerability has been reported in Prevx Pro 2005 that could let local malicious users modify protected files and spoof kernel driver messages. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Prevx Pro File Modification & Driver Spoofing CAN-2005-2144 CAN-2005-2145	Medium	Secunia, Advisory: SA15885, July 1, 2005
SSH Communications Security SSH Secure Shell and Tectia Server V4.3.1	A host key disclosure vulnerability has been reported in SSH Secure Shell and SSH Tectia Server that could let local/ remote malicious users pretend to be other servers. Update to version 4.3.2, http://www.ssh.com/support/downloads/tectia-server/updates-and-packages-4-3.html There is no exploit code required.	SSH Secure Shell and Tectia Server Key Disclosure CAN-2005-2146	Medium	SSH Vulnerability Notification, RQ #11775, June 30, 2005
TCP Chat	A vulnerability has been reported in TCP Chat that could let a remote malicious user perform a Denial of Service. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	TCP Chat Denial of Service CAN-2005-2141	Low	Security Tracker Alert ID: 1014371, July 4, 2005
Veritas Veritas Backup Exec 10.0	Multiple vulnerabilities have been reported in Veritas Backup Exec that could let remote malicious users perform arbitrary code execution, elevate privileges, perform a DoS, or even crash systems. A patch is available from the vendor: http://seer.support.veritas.com/docs/277429.htm **An exploit has been published.**	Veritas Backup Exec Multiple Vulnerabilities CAN-2005-0771 CAN-2005-0772 CAN-2005-0773	High	Secunia, Advisory: SA15789, June 23, 2005 VERITAS Security Advisory VX05-006, VX05-007, VX05-008, June 23, 3005 US-CERT VU#584505, VU#352625, VU#492105 **Security Focus, ID: 14022, June 29, 2005**

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Adobe Acrobat Reader (UNIX) 5.0.10, 5.0.9	A buffer overflow vulnerability has been reported in the 'UnixAppOpenFilePerform()' function due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at: www.adobe.com/products/acrobat/readstep2.html Currently we are not aware of any exploits for this vulnerability.	Adobe Acrobat Reader UnixAppOpen FilePerform Buffer Overflow CAN-2005-1625	High	Adobe Security Advisory, July 5, 2005
Adobe Acrobat Reader (UNIX) 5.0.10, 5.0.9	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user obtain sensitive information. Upgrades avail bale at: www.adobe.com/products/acrobat/readstep2.html There is no exploit code required.	Adobe Reader For Unix Local File Disclosure CAN-2005-1841	Medium	Adobe Security Advisory, July 5, 2005

bzip2 bzip2 1.0.2	A remote Denial of Service vulnerability has been reported when the application processes malformed archives. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.008-openpkg.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-474.html **FreeBSD:** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:14/bzip2.patch** **Conectiva:** **ftp://atualizacoes.conectiva. com.br/** Currently we are not aware of any exploits for this vulnerability.	bzip2 Remote Denial of Service CAN-2005-1260	Low	Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-60, June 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:015, June 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.008, June 10, 2005 RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005 **FreeBSD Security Advisory, FreeBSD-SA-05:14, June 29, 2005** **Conectiva Linux Announce-ment, CLSA-2005:972, July 6, 2005**
bzip2 bzip2 1.0.2 & prior	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions of target files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/b/bzip2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.008-openpkg.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-474.html **FreeBSD:** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:14/bzip2.patch** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** There is no exploit code required.	BZip2 File Permission Modification CAN-2005-0953	Medium	Security Focus, 12954, March 31, 2005 Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005 Debian Security Advisory, DSA 730-1, May 27, 2005 Turbolinux Security Advisory, TLSA-2005-60, June 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.008, June 10, 2005 RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005 **FreeBSD Security Advisory, FreeBSD-SA-05:14, June 29, 2005** **Conectiva Linux Announce-ment, CLSA-2005:972, July 6, 2005**

Centericq Centericq 4.20	A vulnerability has been reported in 'gaduhook::handletoken()' due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	CenterICQ Insecure Temporary File CAN-2005-1914	Medium	Security Focus, 14144, July 5, 2005
Charlton crip 3.5	A vulnerability has been reported due to the creation of temporary files in an insecure manner, which could let a malicious user overwrite files or cause a Denial of Service. Debian: http://security.debian.org /pool/updates/main/c/crip/ There is no exploit code required.	Crip Helper Script Insecure Temporary File Creation CAN-2005-0393	Medium	Debian Security Advisory, DSA 733-1, June 30, 2005
Clam AntiVirus ClamAV 0.x	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the 'cli_scanszdd()' function in 'libclamav/scanners.c' due to a memory and file descriptor leak; and a remote Denial of Service vulnerability was reported in 'libclamav/mspack/mszipd.c' due to insufficient validation of the 'ENSURE_BITS()' macro user-supplied cabinet file header. Upgrades available at: http://prdownloads.source forge.net/clamav/clamav-0.86.1.tar.gz?download Conectiva: ftp://atualizacoes. conectiva.com.br/ Debian: http://security.debian.org/ pool/updates/main/c/clamav/ Currently we are not aware of any exploits for these vulnerabilities.	Clam Anti-Virus ClamAV Remote Denials of Service CAN-2005-1922 CAN-2005-1923	Low	Security Tracker Alert ID: 1014332, June 29, 2005 Conectiva Linux Announce-ment, CLSA-2005:973, July 6, 2005 Debian Security Advisory, DSA 737-1, July 6, 2005
Double Precision Incorporated Courier Mail Server 0.50	A remote Denial of Service vulnerability has been reported in the 'spf.c' source file when processing Sender Policy Framework (SPF) data. Upgrade available at: http://prdownloads.sourceforge.net/ courier/courier-0.50.1.tar.bz2?down load Currently we are not aware of any exploits for this vulnerability.	Courier Mail Server Remote Denial of Service CAN-2005-2151	Low	Secunia Advisory: SA15901, July 4, 2005
Ettercap Ettercap 0.6 .b, 0.6 .a, 0.6.3.1, 0.6.4, 0.6.5, 0.6.6 .6, 0.6.7, 0.6.9, Ettercap-NG 0.7 .0-0.7.2	A format string vulnerability has been reported in the 'curses_msg()' function in the Ncurses interface, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads. sourceforge.net/ettercap/ ettercap-NG-0.7.3.tar.gz?download Currently we are not aware of any exploits for this vulnerability.	Ettercap Remote Format String CAN-2005-1796	High	Secunia Advisory, SA15535, May 31, 2005 **US-CERT VU#286468**
Fores Tent Solutions Log4sh 1.2.3-1.2.5	A vulnerability has been reported in the 'log4sh_readProperties()' function due to the creation of a temporary file in an unsafe manner, which could let a malicious user obtain elevated privileges. Upgrades available at: http://prdownloads. sourceforge.net/log4sh/ log4sh-1.2.6.tgz?use mirror= umn There is no exploit code required.	Log4sh Insecure Temporary File Creation CAN-2005-1915	Medium	Security Tracker Alert ID: 1014374, July 4, 2005
FreeBSD FreeBSD 5.4 -RELEASE	A vulnerability has been reported on Symmetric Multi-Processor (SMP) systems and on Uni Processor (UP) systems with the PREEMPTION kernel option enabled in FreeBSD's ipfw packet filtering code due to insufficient locking on table lookups, which could let a remote malicious user bypass the firewall without authorization. Patch available at:	FreeBSD ipfw Packet Lookup Firewall Bypass CAN-2005-2019	Medium	FreeBSD Security Advisory FreeBSD-SA-05:13, June 29, 2005

	ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:13/ipfw.patch Currently we are not aware of any exploits for this vulnerability.			
FreeBSD FreeBSD 4.x, 5.x	A remote Denial of Service vulnerability has been reported when with an established connection receives and accepts a TCP packet with the SYN flag set. Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:15/tcp4.patch There is no exploit code required.	FreeBSD TCP Stack Established Connection Remote Denial of Service CAN-2005-2068	Low	FreeBSD Security Advisory, FreeBSD-SA-05:15, June 29, 2005
Geeklog Geeklog 1.x	An SQL injection vulnerability has been reported in the user comment retrieval functionality due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code. Updates available at: http://www.geeklog.net/filemgmt/viewcat.php?cid=8 There is no exploit code required.	Geeklog User Comment Retrieval SQL Injection CAN-2005-2152	High	Hardened-PHP Project Security Advisory, July 5, 2005
GlobalNoteScript GlobalNoteScript 4.20 & prior	A vulnerability has been reported in the 'read.cgi' script due to insufficient validation of the 'file' parameter, which could let a remote malicious ser execute arbitrary commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	GlobalNoteScript 'Read.CGI' Remote Command Execution CAN-2005-2165	High	Security Tracker Alert ID: 1014375, July 4, 2005
GNU GNATS 4.1, 4.0	A vulnerability has been reported in gen-index, which could let a malicious user obtain/overwrite arbitrary information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	GNU GNATS Gen-Index Arbitrary Local File Disclosure/Overwrite	High	Security Focus, 14169, July 6, 2005
GNU gzip 1.2.4 a, 1.2.4, 1.3.3-1.3.5	A Directory Traversal vulnerability has been reported due to an input validation error when using 'gunzip' to extract a file with the '-N' flag, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml IPCop: http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:11/gzip.patch OpenPKG: http://www.openpkg.org/	GNU GZip Directory Traversal CAN-2005-1228	Medium	Bugtraq, 396397, April 20, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Security Focus,13290, May 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:11, June 9, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.009, June 10, 2005 RedHat Security Advisory,

	security/OpenPKG-SA-2005.009-openpkg.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Proof of Concept exploit has been published.			RHSA-2005:357-19, June 13, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 **Conectiva Linux Announce-ment, CLSA-2005:974, July 6, 2005**
GNU gzip 1.2.4, 1.3.3	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:11/gzip.patch RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** There is no exploit code required.	GNU GZip File Permission Modification CAN-2005-0988	Medium	Security Focus, 12996, April 5, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:11, June 9, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 **Conectiva Linux Announce-ment, CLSA-2005:974, July 6, 2005**
KPopper KPopper 1.0, 0.93	A vulnerability has been reported in 'popper/popper-send.sh' due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	KPopper Insecure Temporary File Creation CAN-2005-1917	Medium	Secunia Advisory: SA15912, July 5, 2005
Multiple Vendors Apple Safari 1.2-1.2.3, RSS 2.0 pre-release; Omni Group OmniWeb 5.1	A vulnerability has been reported due to a failure to handle scripts securely, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.apple.com/safari/download/ A Proof of Concept exploit has been published.	Multiple Vendors Apple Safari Remote Code Execution CAN-2005-0976	High	Apple Security Advisory, APPLE-SA-2005-04-15, April 16, 2005 **US-CERT VU#998369**
Multiple Vendors OpenLDAP 2.1.25; Padl Software pam_ldap Builds 166, 85, 202, 199, 198, 194, 183-192, 181, 180, 173, 172, 122, 121, 113, 107,	A vulnerability has been reported in OpenLDAP, 'pam_ldap,' and 'nss_ldap' when a connection to a slave is established using TLS and the client is referred to a master, which could let a remote malicious user obtain sensitive information. Trustix:	Multiple Vendors TLS Plaintext Password CAN-2005-2069	Medium	Trustix Secure Linux Advisory, TSLSA-2005-0031, July 1, 2005

105	http://http.trustix.org/pub/trustix/updates/ There is no exploit code required.			
Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian: tp://security.debian.org/pool/updates/main/z/zlib/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch Gentoo: http://security.gentoo.org/glsa/glsa-200507-05.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ Currently we are not aware of any exploits for this vulnerability.	Zlib Compression Library Buffer Overflow CAN-2005-2096	High	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05 , July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice, USN-148-1, July 06, 2005
NetBSD NetBSD 2.0-2.0.2, 1.6-1.6.2	A Denial of Service vulnerability has been reported in the clcs and emuxki audio drivers. Patches available at: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2005-002.txt.asc Currently we are not aware of any exploits for this vulnerability.	NetBSD CLCS / EMUXKI Audio Driver Local Denial of Service CAN-2005-2134	Low	NetBSD Security Advisory, NetBSD-SA2005-002, June 30, 2005
Net-SNMP Net-SNMP 5.2.1, 5.2, 5.1-5.1.2, 5.0.3 -5.0.9, 5.0.1	A remote Denial of Service vulnerability has been reported when handling stream-based protocols. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=12694&package_id =11571&release_id=338899 Currently we are not aware of any exploits for this vulnerability.	Net-SNMP Protocol Denial Of Service	Low	Secunia Advisory: SA15930, July 6, 2005
oftpd oftpd 0.3.0 -0.3.7	A buffer overflow vulnerability has been reported when an overly long argument is submitted for the 'USER' command, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	OFTPD User Command Buffer Overflow	High	Security Focus, 14161, July 6, 2005
phpPgAdmin phpPgAdmin 3.5.3, 3.4.1, 3.1-3.4	A Directory Traversal vulnerability has been reported due to a failure to filter directory traversal sequences from requests to the login form, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPPGAdmin Login Form Directory Traversal	Medium	Security Focus, 14142, July 5, 2005
PHPTools4U.com Eskuel 1.0.2	A vulnerability has been reported due to improper authentication of user credentials, which could let a remote malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required.	Eskuel Unauthorized Administrator Access	High	Security Focus,14163, July 6, 2005
Raxnet Cacti prior to 0.8.6f	Multiple SQL injection vulnerabilities have been reported in the input filters due to insufficient sanitization of user-supplied input before using in SQL queries, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was	RaXnet Cacti Multiple Vulnerabilities CAN-2005-2148	High	Hardened - PHP Project Security Advisory, July 1, 2005

	reported in the 'graph_image.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported because 'session_start()', and 'addslashes()' can be prevented from being called due to a design error, which could let a remote malicious user obtain administrative access. Upgrades available at: http://www.cacti.net/download_cacti.php There is no exploit code required.	CAN-2005-2149		
Rob Flynn Gaim prior to 1.3.1	Several vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported when using the Yahoo! protocol to download a file; and a remote Denial of Service vulnerability was reported in the MSN Messenger service when a malicious user submits a specially crafted MSN message. Updates available at: http://gaim.sourceforge.net/downloads.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200506-11.xml Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-518.html **Debian: http://security.debian.org/pool/updates/main/g/gaim/** There is no exploit code required.	Gaim Remote Denial of Services CAN-2005-1269 CAN-2005-1934	Low	Secunia Advisory, SA15648, June 10, 2005 Ubuntu Security Notice USN-139-1, June 10, 2005 Gentoo Linux Security Advisory, GLSA 200506-11, June 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:099, June 14, 2005 Fedora Update Notifications, FEDORA-2005-410, & 411, June 17, 2005 RedHat Security Advisory, RHSA-2005:518-03, June 16, 2005 **Debian Security Advisory, DSA 734-1, July 5, 2005**
Royal Institute of Technology Heimdal 0.6-0.6.4, 0.5.0-0.5.3, 0.4 a-f	Multiple buffer overflow vulnerabilities have been reported in the 'getterminaltype()' function due to a boundary error in telnetd, which could let a remote malicious user execute arbitrary code. Upgrades available at: ftp://ftp.pdc.kth.se/pub/heimdal/src/heimdal-0.6.5.tar.gz **Gentoo: http://security.gentoo.org/glsa/glsa-200506-24.xml** **SUSE: ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Heimdal TelnetD Remote Buffer Overflow CAN-2005-2040	High	Secunia Advisory, SA15718, June 20, 2005 **Gentoo Linux Security Advisory, GLSA 200506-24, June 29, 2005** **SUSE Security Announcement, SUSE-SA:2005:040, July 6, 2005**
Sendmail Consortium Sendmail 8.8.8 , 8.9 .0-8.9.2, 8.10-8.10.2, 8.11-8.11.7, 8.12.1-8.12.9, 8.12.11	A remote Denial of Service vulnerability has been reported in the milter interface due to the configuration of overly long default timeouts. **SUSE: ftp://ftp.SUSE.com/pub/SUSE** **Debian: http://security.debian.org/pool/updates/main/c/clamav/** There is no exploit code required.	Sendmail Milter Remote Denial of Service CAN-2005-2070	Low	Security Focus, 14047, June 23 **SUSE Security Announcement, SUSE-SA:2005:038, June 29, 2005** **Debian Security Advisory, DSA 737-1, July 6, 2005**
Sun Micro-systems, Inc. Solaris 10.0, 9.0 _x86, 9.0	A vulnerability has been reported in LD_AUDIT,' which could let a malicious user obtain superuser privileges. **Workaround and patch information available at: http://sunsolve.sun.com/**	Sun Solaris Runtime Linker 'LD_AUDIT' Elevated Privileges CAN-2005-2072	High	Security Focus, 14074, June 28, 2005 **Sun(sm) Alert Notification, 101794, June 28, 2005**

	search/document.do?assetkey=1-26-101794-1 **An exploit script has been published.**			
Todd Miller Sudo 1.6-1.6.8, 1.5.6-1.5.9	A race condition vulnerability has been reported when the sudoers configuration file contains a pseudo-command 'ALL' that directly follows a users sudoers entry, which could let a malicious user execute arbitrary code. Upgrades available at: http://www.sudo.ws/sudo/dist/sudo-1.6.8p9.tar.gz OpenBSD: http://www.openbsd.org/errata.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sudo/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Mandriva: http://www.mandriva.com/security/advisories OpenPKG: ftp://ftp.openpkg.org/release/ Gentoo: http://security.gentoo.org/glsa/glsa-200506-22.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-535.html** **Debian:** **http://security.debian.org/pool/updates/main/s/sudo/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** There is no exploit code required.	Todd Miller Sudo Local Race Condition CAN-2005-1993	High	Security Focus, 13993, June 20, 2005 Ubuntu Security Notice, USN-142-1, June 21, 2005 Fedora Update Notifications, FEDORA-2005-472 & 473, June 21, 2005 Slackware Security Advisory, SSA:2005-172-01, June 22, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:103, June 22, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.012, June 23, 2005 Gentoo Linux Security Advisory, GLSA 200506-22, June 23, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 SUSE Security Announce-ment, SUSE-SA:2005:036, June 24, 2005 Turbolinux Security Advisory, TLSA-2005-73, June 28, 2005 **RedHat Security Advisory, RHSA-2005:535-06, June 29, 2005** **Debian Security Advisory, 735-1, July 1, 2005** **Conectiva Linux Announce-ment, CLSA-2005:976, July 6, 2005**
Vipul Razor-agents prior to 2.72	Two vulnerabilities have been reported that could let malicious users cause a Denial of Service. This is due to an unspecified error in the preprocessing of certain HTML and an error in the discovery logic. Updates available at: http://prdownloads.sourceforge.net/razor/razor-agents-2.72.tar.gz?down load Gentoo: http://security.gentoo.org/glsa/glsa-200506-17.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/	Vipul Razor-agents Denials of Service CAN-2005-2024	Low	Security Focus, Bugtraq ID 13984, June 17, 2005 Gentoo Linux Security Advisory, GLSA 200506-17, June 21, 2005 SUSE Security Announce-ment, SUSE-SA:2005:035, June 23, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 **Debian Security Advisory, DSA 738-1, July 5,2 005**

	Debian: **http://security.debian.org/pool/updates/main/r/razor/** Currently we are not aware of any exploits for these vulnerabilities.			
Wojtek Kaniewski ekg 2005-06-05 22:03	A vulnerability has been reported in 'contrib/scripts/linki.py' due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	Wojtek Kaniewski EKG Insecure Temporary File Creation CAN-2005-1916	Medium	Secunia Advisory: SA15889, July 5, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apache Software Foundation Apache prior to 2.1.6	A vulnerability has been reported because a remote malicious user can submit a specially crafted request with both a 'Transfer-Encoding: chunked' header and a 'Content-Length' header to cause Apache to forward the reassembled request with the original Content-Length HTTP header value. Upgrades available at: http://httpd.apache.org/download.cgi There is no exploit code required; however, Proofs of Concept exploits have been published.	Apache HTTP Request Smuggling CAN-2005-2088	High	Security Tracker Alert ID: 1014323, June 29, 2005
Apache Software Foundation Tomcat 4.1.24, 5.0.19	A vulnerability has been reported If the web server is used in conjunction with a proxy server or application gateway (e.g., cache, firewall) and it there is an input validation vulnerability in the web server or one of its applications, then a remote malicious user can use HTTP request smuggling techniques. No workaround or patch available at time of publishing A Proof of Concept exploit has been published.	Apache Tomcat HTTP Request Smuggling CAN-2005-2090	Medium	Security Tracker Alert ID: 1014365, July 3, 2005
AutoIndex PHP Script AutoIndex PHP Script 1.5.2	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'search' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing There is no exploit code required; however, a Proof of Concept exploit has been published.	AutoIndex PHP Script Index.PHP Cross-Site Scripting CAN-2005-2163	High	Security Focus, 14154, July 5, 2005
BEA Systems Weblogic 8.1 SP1	A vulnerability has been reported If the web server is used in conjunction with a proxy server or application gateway (e.g., cache, firewall) and it there is an input validation vulnerability in the web server or one of its applications, then a remote malicious user can use HTTP request smuggling techniques. No workaround or patch available at time of publishing A Proof of Concept exploit has been published.	BEA WebLogic HTTP Request Smuggling CAN-2005-2092	Medium	Security Tracker Alert ID: 1014366, July 3, 2005
Cisco Systems IOS 12.x, R12.x	A vulnerability has been reported in the AAA (Authentication, Authorization, and Accounting) RADIUS authentication method due to an error, which could let a remote malicious user bypass authentication and obtain unauthorized access. Patch information available at: http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml There is no exploit code required.	Cisco IOS AAA RADIUS Authentication Bypass CAN-2005-2105	Medium	Cisco Security Advisory, cisco-sa-20050629-aaa, June 29, 2005
Clam AntiVirus ClamaAV 0.x	A Denial of Service vulnerability has been reported in the Quantum decompressor due to an unspecified error. Updates available at: http://prdownloads.sourceforge.net/clamav/clamav- Gentoo:	ClamAV Quantum Decompressor Denial of Service CAN-2005-2056	Low	Secunia Advisory, SA15811, June 24, 2005 Trustix Security Advisory, TSLSA-2005-0029, June 24, 2005 Gentoo Linux Security

	http://security.gentoo.org/glsa/glsa-200506-23.xml Trustix: http://http.trustix.org/pub/trustix/updates/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Debian:** **http://security.debian.org/pool/updates/main/c/clamav/** Currently we are not aware of any exploits for this vulnerability.			Advisory, GLSA 200506-23, June 27, 2005 **SUSE Security Announcement, SUSE-SA:2005:038, June 29, 2005** **Debian Security Advisory, DSA 737-1, July 6, 2005**
Comdev Software eCommerce 3.1, 3.0	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of the 's_type' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the administration section due to an input validation error, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required.	Comdev eCommerce Review Cross-SIte Scripting & Script Insertion CAN-2005-2138	High	Secunia Advisory: SA15865, June 30, 2005
Community Link Community Link Pro Login.cgi	A vulnerability has been reported in 'login.cgi' due to insufficient sanitization of the 'file' parameter before using in an 'open()' call, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Community Link Pro Input Validation CAN-2005-2111	High	Security Tracker Alert ID: 1014345, June 30, 2005
Covide Groupware-CRM covide 5.2	An SQL injection vulnerability has been reported due to insufficient sanitization of the user ID, which could let a remote malicious user execute arbitrary SQL code. Update available at: http://sourceforge.net/project/showfiles.php?group_id=98036 Currently we are not aware of any exploits for this vulnerability.	Covide Groupware-CRM SQL Injection CAN-2005-2164	High	Secunia Advisory: SA15926, July 6, 2005
DeleGate.org DeleGate Proxy 8.9.2	A vulnerability has been reported when a specially crafted request that contains two 'Content-Length' headers is submitted, which could let a remote malicious user conduct HTTP request smuggling attacks. No workaround or patch available at time of publishing A Proof of Concept exploit has been published.	DeleGate Proxy HTTP Request Smuggling	Medium	Security Tracker Alert ID: 1014359, July 2, 2005
Drupal Drupal 4.6.1, 4.6 , 4.5-4.5.3	A vulnerability has been reported due to insufficient sanitization of user-supplied input to 'comments' and postings,' which could let a remote malicious user execute arbitrary PHP code. Upgrades available at: http://drupal.org/files/projects/drupal-4.5.4.tar.gz There is no exploit code required.; however, a Proof of Concept exploit script has been published.	Drupal Arbitrary PHP Code Execution CAN-2005-2106	High	Security Focus, 14110, June 30, 2005
EtoShop Dynamic Biz Website Builder (QuickWeb) 1.0	An SQL injection vulnerability has been reported in 'verify.asp' due to insufficient sanitization of the 'T1' and 'T2' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Dynamic Biz Website Builder Admin Login SQL Injection CAN-2005-2135	High	Secunia Advisory: SA15818 , June 28, 2005
FrozenPlague Plague News System 0.7	Several vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient of the 'cid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the 'delete.php' script due to insufficient authentication, which could let a remote malicious user bypass security. No workaround or patch available at time of publishing.	Plague News System SQL Injection, Cross-SIte Scripting & Security Bypass CAN-2005-2166 CAN-2005-2167 CAN-2005-2168	High	Secunia Advisory: SA15902 , July 4, 2005

	There is no exploit code required; however, Proofs of Concept exploits have been published.			
FSboard FSboard 2.0	A Directory Traversal vulnerability has been reported which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	FSboard Directory Traversal CAN-2005-2140	Medium	Security Focus, 14111, June 30, 2005
Gossamer Threads Gossamer ThreadsLinks-SQL 3.0-3.0.3	Vulnerabilities have been reported in 'user.cgi' due to insufficient sanitization of the 'Email' parameter and in 'add.cgi' due to insufficient sanitization of various parameters, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.gossamer-threads.com/scripts/links-sql/download.htm There is no exploit code required.	Gossamer Threads Links Multiple HTML Injection	High	Secunia Advisory: SA15319, July 6, 2005
IBM IBM Lotus Notes 6.5-6.5.4, 6.0-6.0.5, 5.0.12, 5.0.3	An input validation vulnerability has been reported because HTML and JavaScript attached to received email messages is executed automatically when viewing the email, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing A Proof of Concept exploit script has been published.	IBM Lotus Notes Script Execution	High	Security Focus, 14164, July 6, 2005
IBM WebSphere 5.0, 5.1	A vulnerability has been reported If the web server is used in conjunction with a proxy server or application gateway (e.g., cache, firewall) and it there is an input validation vulnerability in the web server or one of its applications, then a remote malicious user can use HTTP request smuggling techniques. No workaround or patch available at time of publishing A Proof of Concept exploit has been published.	IBM WebSphere HTTP Request Smuggling CAN-2005-2091	Medium	Security Tracker Alert ID: 1014367, July 3, 2005
Internet Download Manager Corp. Internet Download Manager 4.00-4.05, 3.x, 2.x	A buffer overflow vulnerability has been reported due to improper bounds checking of input data prior to copying into a fixed size memory buffer, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing A Proof of Concept exploit script has been published.	Internet Download Manager Buffer Overflow	High	Security Focus, 14159, July 6, 2005
JAWS JAWS 0.5-0.5.2, 0.4, 0.3, 0.2	Several vulnerabilities have been reported: a vulnerability has been reported in 'BlogModel.php' due to insufficient verification of the 'path' parameter before using to include files, which could let a remote malicious user execute arbitrary code; and a vulnerability has been reported in the 'XML-RPC' library due to an input validation error, which could let a remote malicious user execute arbitrary PHP code. Update available for the input validation vulnerability at: http://www.jaws.com.mx/index.php...ticPage&action=Page&id=2 There is no exploit code required.	Jaws File Inclusion & XML-RPC PHP Code Execution	High	Secunia Advisory: SA15922, July 6, 2005
JBoss Group jBPM 2.0	Several vulnerabilities have been reported: a vulnerability was reported in HSQLDB support, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in the 'org.jboss.web.WebServer' class when a remote malicious user submits a specially crafted HTTP request, which could lead to the disclosure of sensitive information. No workaround or patch available at time of publishing A Proof of Concept exploit has been published for the information disclosure vulnerability.	JBoss jBPM Remote Arbitrary Code Execution & Information Disclosure CAN-2005-2158	High	Security Tracker Alert ID: 1014370, July 3, 2005
Kaf Oseo Quick & Dirty PHPSource Printer 1.0, 1.1	A Directory Traversal vulnerability has been reported in the 'source.php' script due to insufficient validation of the 'file' parameter, which could let a remote malicious user obtain sensitive information. Upgrade available at: http://guff.szub.net/wp-content/sourceprt.zip There is no exploit code required; however, a Proof of Concept exploit has been published.	Quick & Dirty PHPSource Printer Directory Traversal CAN-2005-2169	Medium	Security Tracker Alert ID: 1014376, July 4, 2005

Mambo Mambo Open Source 4.5.2, 4.5.2 .1, 4.5.1 (1.0.9), 4.5.1 Beta 2, 4.5.1 Beta, 4.5.1 , 4.5 (1.0.3beta), 4.5 (1.0.3), 4.5 (1.0.2), 4.5 (1.0.1), 4.5 (1.0.0), 4.0.14	Multiple vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain unauthorized access; and a session ID vulnerability has been reported due to insufficient sanitization of user-supplied input. Upgrades available at: http://mamboforge.net/frs/download.php/6151/MamboV4.5.2.3-stable.tar.gz There is no exploit code required.	Mambo Open Source Multiple Unspecified Injection Vulnerabilities	Medium	Security Focus, 14117 & 14119, June 30, 2005
Mark Kronsbein MyGuestBook 0.6.1	A vulnerability has been reported in the 'form.inc.php3' script due to insufficient validation of the 'lang' parameter before using to include files, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing There is no exploit code required; however, a Proof of Concept exploit has been published.	MyGuestbook 'Form.Inc.PHP3' Remote File Include CAN-2005-2162	High	SoulBlack - Security Research Security Advisory, July 5, 2005
Mozilla.org Mozilla Browser Suite prior to 1.7.6 ; Thunderbird prior to 1.0.2 ; Firefox prior to 1.0.2	A buffer overflow vulnerability has been reported due to a boundary error in the GIF image processing of Netscape extension 2 blocks, which could let a remote malicious user execute arbitrary code. Mozilla Browser Suite; http://www.mozilla.org/products/mozilla1.x/ Thunderbird: http://download.mozilla.org/?product=thunderbird-1.0.2&os=win&lang=en-US Firefox: http://www.mozilla.org/products/firefox/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123 FedoraLegacy: http://download.fedoralegacy.org/redhat/ **An exploit script has been published.**	Mozilla Suite/ Firefox/ Thunderbird GIF Image Processing Remote Buffer Overflow CAN-2005-0399	High	Mozilla Foundation Security Advisory 2005-30, March 23, 2005 US-CERT VU#557948 Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005 **Security Focus, 12881, July 5, 2005**
Multiple Vendors Xoops 2.0.10-2.0.12, 2.0.9 .3, 2.0.9.2, 2.0.5-2.0.5.2, 2.0- 2.0.3; XML-RPC for PHP XML-RPC for PHP 1.1, 1.0.99 .2, 1.0.99, 1.0-1.02; WordPress 1.5-1.5.1 .2, 1.2-1.2.2, 0.71,0.7; S9Y Serendipity 0.8.1, 0.8 -beta6 Snapshot, 0.8 -beta5 & beta6, 0.8; PostNuke Development Team PostNuke 0.76 RC4a&b, RC4, 0.75; phpMyFAQ 1.5 RC1-RC4, 1.5 beta1-beta3, 1.5 alpha1&2, 1.4-1.4.8, 1.4; PEAR XML_RPC 1.3 RC1-RC3, 1.3; MandrakeSoft Linux Mandrake 10.2 x86_64, 10.2, 10.1 x86_64, 10.1 , 10.0 amd64, 10.0, Corporate Server 3.0 x86_64, 3.0; Drupal 4.6.1, 4.6, 4.5- 4.5.3	A vulnerability was reported due to insufficient sanitization of the 'eval()' call, which could let a remote malicious user execute arbitrary PHP code. Drupal: http://drupal.org/files/projects/drupal-4.5.4.tar.gz Mandriva: http://www.mandriva.com/security/advisories Pear: http://pear.php.net/get/XML_RPC-1.3.1.tgz PhpMyFaq: http://freshmeat.net/redir/phpmyfaq/38789/url_zip/download.php S9Y Serendipity: http://prdownloads.sourceforge.net/php-blog/serendipity-0.8.2.tar.gz?d ownload WordPress:	Multiple Vendors XML-RPC for PHP Remote Code Injection CAN-2005-1921	High	Security Focus, 14088, June 29, 2005 Gentoo Linux Security Advisory, GLSA 200507-01, July 3, 2005 Fedora Update Notifications, FEDORA-2005-517 & 518, July 5, 2006 Ubuntu Security Notice, USN-147-1 & USN-147-2, July 05 & 06, 2005 **US-CERT VU#442845**

	http://wordpress.org/ latest.zip XML-RPC: http://prdownloads. sourceforge.net/ phpxmlrpc/xmlrpc-1.1.1.tgz?download Xoops: http://www.xoops.org/ modules/core/ visit.php?cid=3&lid=62 Gentoo: http://security.gentoo.org/ glsa/glsa-200507-01.xml Fedora: http://download.fedora. redhat.com/pub/fedora/ linux/core/updates/ Trustix: http://http.trustix.org/pub/ trustix/updates/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/p/php4/ Currently we are not aware of any exploits for this vulnerability.			
NaboCorp Softwares NaboPoll 1.2	A vulnerability has been reported in 'survey.inc.php' due to insufficient verification of the 'path' parameter before used to include files, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	NaboCorp Softwares NaboPoll Remote File Include CAN-2005-2157	High	Security Tracker Alert ID: 101435, July 2, 2005
NashTech EasyPHPCalendar 6.1.5 & prior	A vulnerability has been reported due to insufficient verification of the 'serverPath' parameter before used to include files, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	EasyPHPCalendar 'serverPath' File Inclusion CAN-2005-2155	High	Secunia Advisory: SA15893, July 5, 2005
Nate.com NateOn Messenger 3.0	A vulnerability has been reported due to an input validation error, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploit for this vulnerability.	NateOn Messenger Information Disclosure CAN-2005-2137	Medium	Secunia Advisory: SA15819, June 29, 2005
Oracle Corporation Application Server Web Server 9.0.2	A vulnerability has been reported If the web server is used in conjunction with a proxy server or application gateway (e.g., cache, firewall) and it there is an input validation vulnerability in the web server or one of its applications, then a remote malicious user can use HTTP request smuggling techniques. No workaround or patch available at time of publishing A Proof of Concept exploit has been published.	Oracle Application Server Web Server HTTP Request Smuggling CAN-2005-2093	Medium	Security Tracker Alert ID: 1014368 , July 3, 2005
Oracle Corporation Oracle Application Server Web Cache 9.0.2	A vulnerability has been reported when a specially crafted request that contains two 'Content-Length' headers is submitted, which could let a remote malicious user conduct HTTP request smuggling attacks. No workaround or patch available at time of publishing A Proof of Concept exploit has been published.	Oracle Application Server Web Cache HTTP Request Smuggling	Medium	Security Tracker Alert ID: 1014360 , July 2, 2005
OSTicket osTicket STS 1.3 beta, 1.2.7, 1.2	Several vulnerabilities have been reported: a vulnerability was reported in the 'class.ticket.php' script due to insufficient validation, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in the 'view.php' and 'open.php' scripts because the 'inc' variable is not properly defined, which could let a remote malicious user include and execute arbitrary PHP files. No workaround or patch available at time of publishing There is no exploit code required; however, a Proof of Concept exploit has been published.	OSTicket Multiple Input Validation CAN-2005-2153 CAN-2005-2154	High	RST / GHC Advisory, July 1, 2005

Pavsta Pavsta Auto Site	A vulnerability has been reported in 'user_check.php' due to insufficient verification of the 'sitepath' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	Pavsta Auto Site 'user_check.php' Arbitrary Code Execution CAN-2005-2139	High	Security Tracker Alert ID: 1014321, June 29, 2005
PHPGroupWare PHPGroupWare 0.9.14 .007	An unspecified vulnerability has been reported in the addressbook. The impact was not specified. Upgrade available at: p://prdownloads.sourceforge.net/phpgroupware/phpgroupware-0.9.16.00 2.tar.gz Currently we are not aware of any exploits for this vulnerability.	PHPGroupWare Addressbook	Not Specified	Security Focus, 14141, July 5, 2005
PHPNews PHPNews 1.2.5	An SQL injection vulnerability has been reported in the 'news.php' script due to insufficient sanitization of the 'prevnext' parameter before used in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrade available at: http://prdownloads.sourceforge.net/newsphp/phpnews_1-2-6.zip?download There is no exploit code required.	PHPNews 'News.PHP' SQL Injection CAN-2005-2156	High	Security Focus, 14133, July 4, 2005
PlanetDNS PlanetFileServer Standard (BETA)	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a vulnerability was reported in 'delete.php' due to insufficient sanity checks on deletion requests, which could let a remote malicious user bypass access restrictions. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PlanetDNS PlanetFileServer Remote Buffer Overflow & Access Restriction Bypass CAN-2005-2159	High	Security Focus, 14138 & 14139, July 4, 2005
QuickBlogger QuickBlogger 1.4	A Cross-Site Scripting vulnerability has been reported because HTML code is not filtered from user-supplied input in the 'Your Name' and 'Comments' sections, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	QuickBlogger Cross-Site Scripting	High	EXPL-A-2005-011 Advisory, July 5, 2005
Raritan Dominion SXA-48, SX8, SX4, SX32 2.4.6 firmware, SX32, SX16	Several vulnerabilities have been reported: a vulnerability was reported in '/etc/shadow/ because the default file permission is set to world-readable, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported in '/bin/busybox/ because the file permission is set to world-writable, which could let a remote malicious user move/delete the file and potentially execute arbitrary code. Updates available at: http://www.raritan.com/support/sup_upgrades.aspx There is no exploit code required.	Raritan Dominion SX Multiple Vulnerabilities CAN-2005-2136	High	Secunia Advisory: SA15853, June 29, 2005
Raven Software Soldier Of Fortune 2 1.0 3, 2 1.0 2	A remote Denial of Service vulnerability has been reported in the '/ignore' command when a client ID is submitted that is larger than 1024. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Raven Software Soldier Of Fortune 2 Remote Denial of Service CAN-2005-2115	Low	Secunia Advisory: SA15868, June 30, 2005
Real Networks RealPlayer G2, 6.0 Win32, 6.0, 7.0 Win32, 7.0 Unix, 7.0 Mac, 8.0 Win32, 8.0 Unix, 8.0 Mac, 10.0 BETA, 10.0 v6.0.12.690, 10.0, 0.5 v6.0.12.1059 10.5 v6.0.12.1056, v6.0.12.1053, v6.0.12.1040, 10.5 Beta v6.0.12.1016, 10.5, 10 Japanese, German, English, 10 for Linux, 10 for Mac OS Beta, 10 for Mac OS 10.0.0.325, 10 for Mac OS 10.0.0.305, 10 for Mac OS, 10 for Mac OS 10.0 v10.0.0.331, RealPlayer 8, RealPlayer Enterprise 1.1, 1.2, 1.5-1.7, RealPlayer For Unix 10.0.3, 10.0.4,	A vulnerability has been reported when a specially crafted media file is opened, which could let a remote malicious user execute arbitrary code. RealNetworks: http://service.real.com/help/faq/security/050623_player/EN/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-517.html http://rhn.redhat.com/errata/RHSA-2005-523.html	RealNetworks RealPlayer Unspecified Code Execution CAN-2005-1277 CAN-2005-1766	High	eEye Digital Security Advisory, EEYEB-20050504, May 5, 2005 RedHat Security Advisories, RHSA-2005: 517-02 & RHSA-2005: 523-05, June 23, 2005 Fedora Update Notifications, FEDORA-2005-483 &

RealPlayer for Windows 7.0, RealPlayer Intranet 7.0, 8.0	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Gentoo:** **http://security.gentoo.org/glsa/glsa-200507-04.xml** Currently we are not aware of any exploits for this vulnerability.			484, June 25, 2006 SUSE Security Announcement, SUSE-SA:2005:037, June 27, 2005 **Gentoo Linux Security Advisory, GLSA 200507-04, July 6, 2005**
Sun Microsystems, Inc. SunONE Web Server 6.1 SP4	A vulnerability has been reported If the web server is used in conjunction with a proxy server or application gateway (e.g., cache, firewall) and it there is an input validation vulnerability in the web server or one of its applications, then a remote malicious user can use HTTP request smuggling techniques. No workaround or patch available at time of publishing A Proof of Concept exploit has been published.	SunONE Web Server HTTP Request Smuggling CAN-2005-2094	Medium	Security Tracker Alert ID: 1014369, July 3, 2005
Sun Microsystems, Inc. Sun Java System Web Proxy Server 3.6 SP4	A vulnerability has been reported when a specially crafted request that contains two 'Content-Length' headers is submitted, which could let a remote malicious user conduct HTTP request smuggling attacks. No workaround or patch available at time of publishing A Proof of Concept exploit has been published.	Sun Java System Web Proxy Server HTTP Request Smuggling	Medium	Security Tracker Alert ID: 1014358, July 2, 2005
Thierry Nkaoua News-tnk 1.2 1 & prior	A Cross-Site Scripting vulnerability has been reported in the WEB parameter, which could let a remote malicious user execute arbitrary JavaScript code. Upgrade available at: http://www.linux-sottises.net/software/news-tnk_v1.2.3.tar.gz Currently we are not aware of any exploits for this vulnerability.	News-TNK Unspecified Security Vulnerability CAN-2002-0458	High	Security Focus, 14145, July 5, 2005
Xoops Xoops 2.x	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'comment_edit.php' due to insufficient sanitization of the 'cid' parameter and in 'edit.php' due to insufficient sanitization of the 'order' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in the XML-RPC interface due to insufficient sanitization of user-supplied, input, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: prdownloads.sourceforge.net/xoops/Xoops-2.0.12.zip?download There is no exploit code required; however, Proofs of Concept exploits have been published.	Xoops Cross-Site Scripting & SQL Injection CAN-2005-2112 CAN-2005-2113	High	Secunia Advisory: SA15843, June 30, 3005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **New Wireless Broadband Technology Touted:** Backers of a narrow band wireless technology that uses low frequencies alongside existing activity on the wireless transmission spectrum claim better reach than next generation WiMax wireless, with a lower cost because of the sub-gigahertz spectrum and low power required for the solution. Source: http://www.technewsworld.com/story/8OGbT3UKPWiiC4/New-Wireless-Broadband-Technology-Touted.xhtml.
- **Threat From Mobile Device Viruses a Sleeping Giant:** Communication security experts do not all agree that cell phone and mobile device viruses pose imminent threats to U.S. consumers. Whether virus attacks become a problem in six months or five years might depend on how cell phone carriers react now to the threat potential. Source: http://www.technewsworld.com/story/44222.html.

Wireless Vulnerabilities

- **Symbian Trojan drains the life from phones:** Virus writers have created a new Symbian Trojan called Doomboot-A that loads an earlier mobile virus (Commwarrior-B) onto vulnerable smartphones. Doomboot-A also preventing infected phones from booting up properly. This cocktail of viral effects spells extra trouble for Symbian Series 60 smartphone users, especially those who play around with pirated games. Source: http://www.theregister.co.uk/2005/07/04/symbian_trojan_doomboot/

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
July 6, 2005	dlm.c	No	Proof of Concept exploit for the Internet Download Manager Buffer Overflow vulnerability.
July 6, 2005	malmail.txt	No	Proof of Concept exploit for the IBM Lotus Notes Script Execution vulnerably.
July 5, 2005	druppy461.pl	Yes	Proof of Concept exploit for the Drupal Arbitrary PHP Code Execution vulnerability.
July 5, 2005	firesnake.c	Yes	Script that exploits the Mozilla Suite/ Firefox/ Thunderbird GIF Image Processing Remote Buffer Overflow vulnerability.
July 5, 2005	Schily-Root.tar	Yes	Proof of Concept exploit for the Sun Solaris Runtime Linker 'LD_AUDIT' Elevated Privileges vulnerability.
July 1, 2005	ieCrash-javaprxy.txt	Yes	Proof of Concept Denial of Service exploit for the Microsoft Internet Explorer Arbitrary Code Execution vulnerability.
July 1, 2005	knock-0.5.tar.gz	N/A	A server/client set of tools that implements port-knocking, which is a method of accessing a backdoor to your firewall through a special sequence of port hits.
July 1, 2005	multihtml.c.exploit.txt	No	Exploit for the multihtml.c format string vulnerability.
July 1, 2005	peercast.c	Yes	Script that exploits the Peercast.org PeerCast Remote Format String vulnerability.
July 1, 2005	phpbb2_0_15.pl.txt	Yes	Exploit for the php 2.0.15 viewtopic.php remote command execution vulnerability.
July 1, 2005	prowebExec.txt	No	Details on exploiting the Community Server Forums Cross-Site Scripting vulnerability.
July 1, 2005	winfingerprint-0.6.2.zip	N/A	Win32 Host/Network Enumeration Scanner is capable of performing SMB, TCP, UDP, ICMP, RPC, and SNMP scans. Using SMB, winfingerprint can enumerate OS, users, groups, SIDs, password policies, services, service packs and hotfixes, NetBIOS shares, transports, sessions, disks, security event log, and time of day in either an NT Domain or Active Directory environment.
June 29, 2005	ASPNuke.pl ASPNukeSQL080.txt	No	Exploits for the ASP Nuke SQL Injection & Cross Site Scripting vulnerability.
June 29, 2005	backupexec_agent.pm.txt	No	Veritas Backup Exec Agent CONNECT_CLIENT_AUTH Request exploit that makes use of a stack overflow.
June 29, 2005	clogin.pl	No	Proof of Concept exploit for the Community Link Pro Input Validation vulnerability.
June 29, 2005	communityXSS.txt	No	Exploit for the Community Server Forums Cross-Site Scripting vulnerability.
June 29, 2005	Infradig60.txt	No	Sample Denial of Service exploit for the Infra dig Infra mail Advantage Server Edition Multiple Remote Buffer Overflow vulnerabilities.

[back to top]

Trends

- **Reverse engineering patches making disclosure a moot choice?** In a paper published in early June, SABRE researchers discussed how they had pinpointed, in less than 30 minutes, the flaw fixed by a Microsoft update to the Secure Sockets Layer (SSL). A reliable exploit for the flaw was created in less than 10 hours. In another example in the paper, the tool was used to discover in less the 3 hours that Microsoft had corrected a communications vulnerability in the Internet Security and Acceleration (ISA) Server, but had missed the same vulnerability in other parts of the system. Source: http://www.securityfocus.com/news/11235.
- **Cybercrime cost about $400 billion:** A report that was commissioned by McAfee discusses how organized crime and cyber crime are developing, and looks at the future threat this activity could pose to home computers, government computer networks, and to computer systems in the business sector. The report reveals a hierarchy of cyber criminals, discussing the recent evolution of the amateur cyber delinquent to the professional cyber gang. Source: http://www.crime-research.org/news/06.07.2005/1344/.
- **Exploit for Vulnerability in XML-RPC:** US-CERT is aware of a working public exploit for a vulnerability in a common PHP extension module (XML-RPC) that could allow a remote attacker to execute code of their choosing on a vulnerable system. Any application, typically web-based, that uses a flawed XML-RPC PHP implementation is vulnerable to exploitation. Source: http://www.us-cert.gov/current/.
- **Exploit for Vulnerability in Microsoft's JVIEW Profiler (javaprxy.dll)**: US-CERT is aware of a working public exploit for a vulnerability in the Microsoft JVIEW Profiler (javaprxy.dll) component, an interface to the Microsoft Java Virtual Machine. This vulnerability can be exploited when a user attempts to view an HTML document (e.g., a web page or an HTML email message) that attempts to instantiate the JVIEW Profiler COM object in a certain way. Source: http://www.us-cert.gov/current/.
- **Fake Microsoft Security Bulletin Email:** US-CERT has received reports of an email message circulating purporting to be a Microsoft Security Bulletin. The email directs the user to download and install an executable that is supposed to be a cumulative patch. Through the use of social engineering that attacker is hoping to trick the user into thinking they will be installing a cumulative patch when in fact they are installing a version of SDBot, a commonly used Trojan horse. Source: http://www.us-cert.gov/current/.
- **Hackers crack two-factor security:** IT experts warned that two-factor authentication is not secure enough to stop Internet banking fraud. "Two-factor is good, but hackers are responding," Graham Cluley, senior technology consultant at Sophos, told vnunet.com."The latest generation of spyware not only includes key-loggers that trap passwords, but screen-grabbing software. This takes multiple images of what the user is doing and sends it straight to the hacker." Source: http://www.vnunet.com/vnunet/news/2139253/two-factor-authentication
- **E-mails hit record in May as criminals go phishing:** According to IBM Corporation, the number of phishing attacks soared to a record high in May, as massive volumes of scam e-mails were pumped out by criminals seeking to dupe unsuspecting victims. In May, more than 9.1 million e-mails containing a phishing scam were detected, more than three times the 2.8 million detected in April and 18 per cent higher than the previous record of 7.7 million recorded in January. Source:

http://news.yahoo.com/news?tmpl=story&u=/cpress/20050630/ca_pr_on_tc/ibm_phishing_attacks_2.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win 32 Worm	Slight Increase	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Zafi-D	Win 32 Worm	Increase	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
3	Mytob.c	Win 32 Worm	Decrease	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
4	Netsky-Q	Win 32 Worm	Slight Decrease	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
4	Mytob-BE	Win 32 Worm	New	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
6	Lovgate.w	Win 32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
6	Netsky-Z	Win 32 Worm	Increase	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
6	Mytob-AS	Win 32 Worm	New	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
9	Netsky-D	Win 32 Worm	Decrease	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
10	Mytob-EP	Win 32 Worm	New	June 2005	Another slight variant of the mass-mailing worm that utilizes an IRC backdoor and LSASS vulnerability to propagate. Also propagates by email, harvesting addresses from the Windows address book.

Table Updated July 5, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Hackers unleash industrial spy Trojan:** IT security experts have detected a malware-based hack attack that attempts to gain unauthorized access to the networks of specifically targeted domains.
  Security firm MessageLabs, which discovered the attack, explained that the Trojan targets only a small number of email addresses rather than mass mailing itself to as many recipients as possible.
  The infected emails were transmitted to a highly targeted list of recipients at only four domains, suggesting that the hackers were using the malware for industrial espionage. The attack is designed to exploit a vulnerability in Microsoft Word caused by a buffer overflow when handling macro names. Source: http://www.vnunet.com/vnunet/news/2139033/hackers-unleash-industrial-spy.

[back to top]

Last updated July 07, 2005